U. S. House of Representatives:
Science Committee
"Cyber Security Education:
Meeting the Needs of Technology Workers and Employers"
July 21, 2004

Detailed Testimony

1. Cyber Security Education

Cyber Security Education is the process of informing technology professionals, end-users, managers and researchers about the technical and non-technical aspects of protecting their information resources, and expanding our knowledge in the field. It is a multi-disciplinary field that is both broad and deep. The field is constantly evolving to incorporate more components based on current & historical events and research. The term itself refers both to security aspects as well as to cyber forensics. It requires simultaneous education, training and research in multiple areas (technology, business, management, finance, psychology, computer science, etc.)

a. Components of the Field: Technical, Managerial, Operational

Cyber Security Education is more than just the technical aspect of detecting or eliminating the latest virus, or preventing hacker attacks (the public personae). It requires knowledge of technical areas, addressing management, and how to infuse security practices into the everyday operational aspects of an organization. Technical aspects include firewalls, network security, cryptography and software development.

Managerial components include personnel issues, disaster recovery planning, funding (direct and indirect costs, ROI, payback), the psychology or mind-set of a perpetrator, operational security management, public relations and legal/regulatory components. Operational issues include day-to-day security operations, both for the security field professional and the everyday user.

Each part of the field involves varying levels of research, education and training. Research investigates new technologies, financial issues, approaches to security management, personnel issues and legal/regulatory needs. The most recognizable research is on the technological components of information security.

b. Education vs. Training

Often interchangeably used, education and training differ greatly. Education's goal for the student is multi-purpose: teach them specific technical skills, develop critical thinking and problem-solving abilities, increase the knowledge of the vast background material in the field, improve communication capabilities & information literacy skills, and engage the student in some form of research.

Training is generally focused on a product or specific set of skills in an area. However, at its highest level, some training attempts to approximate education, typically by improving some of a student's background knowledge in a field and/or developing problem solving capabilities.

c. Research and Education

A major methodological issue for a university is whether to focus on research or on classroom education. University reputations are based on faculty research and the institution's research abilities. Johns Hopkins University was the first U.S. university to include research in the educational process. Typically, university research has not been focused specifically in the areas of information security or cyber forensics. Research for these areas is done in various other disciplines that directly or indirectly affect these fields.

d. Emerging Discipline

Because of its breadth, Cyber Security Education is a young field and not currently recognized as a discipline. At the moment it has not yet been accepted as a discipline of its own. It has components in various areas: mathematics, computer science, business, finance, engineering, psychology, law, etc. Consequently, research, education and training occurs in each of these disciplines independently. For example, research in the field of mathematics may result in a better crypto-key system.

2. Programs at JHU

Johns Hopkins has responded to the need for intensive research, education and training in cyber security in all of its academic areas. Some of its programs were in place before the events of Sept 11. However, all schools at the university have implemented or are in the process of implementing, information security education and/or research in their academic disciplines. In addition, Hopkins has created the Johns Hopkins University Information Security Institute whose goals are to foster research in information security, help develop multi-disciplinary approaches to security education, provide seminars and other educational activities, and advance the literature in the field.

a. Internal Programs

Almost all schools at Hopkins have incorporated some form of security education. Depending on the program and level, it could include simple background knowledge about the area and how security applies to the specific educational discipline, or it could include in-depth studies into security approaches in a field, practical applications or advanced security research.

b. Internal Collaboration

Several of Hopkins' Schools have collaborated on academic programs that are interdisciplinary in nature. The flagship program at Hopkins' Information Security Institute is the Masters of Science in Security Informatics (MSSI). It is a collaboration of several schools at Hopkins: Whiting School of Engineering, Krieger School of Arts and Sciences, Bloomberg School of Public Health, Nitze School of Advanced International Studies and the School of Professional Studies in Business and Education. Over 25 full-time, part-time or adjunct faculty are available to deliver the MSSI courses at multiple Hopkins' sites in the Baltimore-Washington area.

In addition, some schools at Hopkins have developed internal collaborations across academic levels. The Whiting School of Engineering and the Krieger School of Arts and Sciences jointly offer a concurrent bachelors/masters program in security. The School of Professional Studies in

Business and Education offers a joint technology bachelors/masters degree, with a concentration in information security.

c. External Collaborations

The School of Professional Studies in Business and Education is in the process of developing joint programs with several area community colleges. These would provide students at 2-year institutions complete academic program opportunities at the bachelor's level, and extending into the master's level.

The joint program offered by the Whiting School of Engineering and the Krieger School of Arts and Sciences includes opportunities for undergraduates of other local universities, which have established agreements with these Hopkins schools.

d. Research, seminars, courses/teaching, publishing

The Johns Hopkins Information Security Institute has become the focal point for information security research at the university. Over 15 full-time faculty or JHU Applied Physics Laboratory researchers are involved in some aspect of information security research.

3. Strengths & Weaknesses of Current Education

a. Education or Training

Often a potential employee seeks the short-term goal of satisfying a potential employer's advertised need, through specific skill-set training. Many potential employees view the requirements indicated in a particular employment ad, then attempt to obtain the specific skill required (CISCO training, CISSP certification, etc.). While potentially valid as an entry into the field, or for specific job requirement, these are not intended to indicate the wider-range of skills and abilities many employers seek.

Education rather than training provides potential employees this wider-set of knowledge and abilities, in addition to specific technology skill sets (not necessarily for a specific product). These include: critical thinking and problem-solving, knowledge of the vast background material in the field, communication, information literacy and some form of research. Often a student in a program wants to know if they will be learning Product-X. The answer is usually that the program may teach you some things about Product-X, but its goal is to teach you how to learn, and apply that skill to learning about different products. At times we may use various products (including Product-X) as examples in our classes or for demonstration purposes, but the goal is not to teach a specific product.

In addition, education is intended to develop the next generation of researchers in a discipline. Because of the nature of the information security field, much of the research is focused in other disciplines. For example, a math researcher may apply their findings to the information security field.

b. Costs:

The cost of education programs covers many components: physical items, facilities management, program development and maintenance, and faculty hiring, training and education.

1. Facilities Set-up and Management

Teaching state-of-the-art information security or cyber forensics programs requires facilities that can handle the technology. This means some form of computer lab capability, typically networked. While the most current technology is not absolutely necessary, the more dated the technology the more difficult it is to get current and potential students and employers to accept a program as useful. It is a constant problem to remain current enough to teach the most important components of security and forensics, and still not spend 'every last dime' on the most recent technology.

An additional component is the style or set-up of lab facilities. Most lab set-ups will be done in one of 2 approaches: a dedicated lab or a multi-purpose lab. Dedicated labs are designed for a specific program, and have minimal impact on other programs or facilities. However, they will sit idle when the specific educational program is not offered. In addition, management of these labs may be easier (for program setup and use), but they are almost always 'locked down', and only allowed for students of the specific program. No other use is allowed because of the sensitive nature of the set-up, and because of the potential problems with other areas. For example, if a lab virus or other destructive software is unintentionally allowed into another lab facility, that facility may become corrupted. If it is a networked facility, others may also become corrupted.

Multi-purpose labs are more functional, but can be much more costly in terms of set-up and management. These labs may need periodic isolation, a special set-up, and additional management. In addition, when they are used by the security or forensic program, disruption to other programs needing the lab will occur. This will include specialized set-up and clean-up time, in addition to the actual class time.

All of these take time, resources and increase costs of program offerings. Hardware costs can range from $500 to $2,000 per machine, plus networking and software costs. Management time will include initial lab set-up, in addition to the individual class set-up and clean-up, depending on the type of lab. While difficult to provide specific cost estimates for this time, it can include several hours of a lab manager's time and up to 1½ days of a support staff person's time, for each class session.

2. Program Development & Maintenance

Development, implementation, operation and maintenance of an educational program can take more than a year. Typically, the process includes:

a. An assessment of the need for graduates of a program
b. Development of an advisory board
c. Identification of program components
d. Internal and external approval steps
e. Organization of the program into modules/courses
f. Development of the course material
g. Advertising/marketing the program
h. Program implementation
i. Constant program evaluation and improvement

While there are ways to speed up the process, each step is needed. In approving such programs, cost is always a major factor. Employment surveys, component development costs, hardware & software identification, developing appropriate course/lesson plans around them, marketing and oversight are the major ones.

3. Faculty

Cost issues for faculty center on the issues of part-time vs. full-time faculty, and the role of faculty in the program. Part-time faculty are usually used for teaching purposes, and to provide expertise in a specific topic area. While they may be involved in program development, they are not typically responsible for program development or success/failure.

Full-time faculty are involved in one or more aspects of program development, implementation, teaching, evaluation. In addition, in many institutions they are involved in research activities. This can be a source of cutting-edge knowledge, prestige and income for the faculty member and institution, but can also create problems. These and other faculty issues are addressed in section 4.a

c. Background Checks

A more recent problem that has surfaced is the issue of student background checks. With the events of September 11, increasingly questions of appropriateness of students in the classroom have arisen. A discussion of background checks raises many additional questions:

1. What is the purpose of the background checks?
2. How deep or wide will they go?
3. How much will they cost?
4. How long will they take?
5. Who will pay for them?
6. Who will do them?
7. What will we do with the information once it is obtained?
8. Will it prevent a student from entering a program or restrict their access to certain courses or material?
9. Are they relevant given the availability of material on the Internet?
10. Are they legal?

Background checks are costly, time consuming and raise legal concerns around privacy and profiling. But, given the awareness of security concerns, additional guidance will be needed in this area.

d. Ethical Agreements

Some programs have instituted ethical agreements with students in specific programs. They attempt to educate the student on the seriousness of the topic, and the expectations of professional and moral behavior that accompany the education. However, enforcement is difficult, especially outside the classroom or after the program is completed.

4. Faculty Preparation, Recruitment and Retention

a. Part-time vs. Full-time Faculty

Identifying appropriate faculty for specialized programs such as information security and cyber forensics is a challenge. Generally, the options are:

1. Design the program around the current full-time faculty knowledge base
2. Upgrade current full-time faculty skills/knowledge
3. Hire new full-time faculty, specifically for this program
4. Hire part-time, practitioner faculty to teach in the program

Designing the program around the current full-time faculty knowledge base is the easiest and least costly approach, but is usually the least desirable. Typically, their knowledge base is very specific and may not cover the broad-range of technical and non-technical topics required. Consequently, the program manager is required to augment the current knowledge base with additional, training or education, or hiring other faculty, either full-time or part-time. In addition, the current faculty knowledge base may already be out-of-date or too narrow.

Upgrading current full-time faculty skills and knowledge is desirable and useful for them, but is time consuming and adds cost to the program development and operation. It may delay the program development and implementation.

Hiring new full-time faculty may be quicker, but also costly. In addition, if the program is not commercially successful (and if they are not involved in research which generates grant income), the organization has incurred the additional faculty cost, with no offsetting income. That may mean the faculty position results in a short-term employment opportunity.

Hiring part-time, practitioner faculty is often difficult and time consuming. While it provides the educational institution the least costly staffing solution, there are many other factors that affect the hiring decision. These faculty often:

1. Are not trained educators
2. Are already employed and consequently have problems with pre-existing course schedules
3. Cannot teach during the day
4. May travel too much
5. May have only some allegiance to the program and/or institution
6. May not have the necessary academic credentials
7. May not have a teaching aptitude

When hiring part-time faculty the organization needs to commit to teaching them to be educators. Learning to educate at the college or university level requires some intensive interaction between the academic program manager and part-time faculty member, and a commitment on the part of the university to provide faculty development in the area of teaching skills and course/classroom management. In addition to creating a syllabus and organizing some lectures, the part-time faculty member will need to learn to manage the classroom environment, create and implement effective and fair evaluation instruments and assign grades. In addition, the faculty will need to evaluate student writing, incorporate critical thinking and problem-solving skills, include information literacy, develop creative presentation styles, and infuse current research into the education process. These can take some time, patience, and

commitment on the organization's part, with no guarantee the part-time faculty member will continue with the program.

In addition, the education organization needs to implement a support system for the part-time faculty member. This includes administrative support for typical needs (copying, book order processing, etc.), and academic support for course content, unexpected problems, articulating college/university policies on various issues and handling grading questions.

b. Teaching vs. Research

In some educational organizations, full-time faculty may also be involved in research activities. While this can provide a terrific resource for the program in terms of up-to-date information in the field, and potential student involvement in the research, it can also create conflicts for the faculty. Research activities are often funded by grants and require intensive time commitments of the faculty. Consequently, less time is available for teaching.

c. Hopkins Approach

Hopkins has implemented a variety of solutions to address faculty issues. In some schools, full-time faculty are involved in both research and teaching. In addition, part-time faculty are used in selected courses or program components to either provide the instruction or assist the full-time faculty member with their instruction.

Others schools at Hopkins are using a large group of part-time faculty who are professionals in their area, to teach in their program. In addition to selecting fully qualified part-time faculty (based on factors such as professional experience, teaching experience, teaching aptitude, academic credentials and availability), they are provided a full range of teaching professional support from both the program manager and other groups with the organization.

5. Federal Government Assistance

a. Funding NSF Initiatives

The National Science Foundation (NSF) has attempted to provide several opportunities to fund information security educational initiatives. Because of funding issues NSF has not been able to support innovative initiatives in information security education. Providing more complete funding for the NSF initiatives will help in the development of different and more complete academic programs.

b. SFS Graduates

Evidently, one of the issues with the Scholarship for Service (SFS) program is the ability of government agencies to absorb the number of graduates. Some may need assistance in developing their plans and/or finding ways to hire the graduating talent. Others, (DOD, NSA, etc.) have indicated a strong need for qualified SFS graduates. One issue here may be the ability of the students to obtain appropriate security clearances.

c. Development as a Discipline

Provide some funding to encourage the development of information security and cyber forensics as disciplines. This would encourage faculty to enter the field, develop research incentives, and

provide money for the development applied and research-based academic programs. In addition, it would bring together research and education that is pertinent to the field.

d. Non-SFS Scholarships

Working with the private sector and state governments, the Federal Government can help to develop scholarship programs to provide educational funding for students who may want to be employed in one of these areas. The private sector and state governments have as strong a need for information security professionals as the Federal Government. In some instances they may be on the front lines, or provide early-warning notification to the Federal Government. Consequently, they need as much education in the security area as the Federal Government.

6. Other Issues

In addition to the request information areas, these additional topics may be of interest:

a. Defining Educational Standards

Developing educational standards in a discipline helps define it as a discipline. The defining of such standards would help the fields of information security and cyber forensics. While simple in concept, it is more difficult in practice. It would require the defining of security knowledge needs in various professions, and at different levels within a profession. For example, in a given industry there are system end-users, managers, technical staff and researchers. Each requires different levels and types of security education and skills. The end-user may need to understand how, and a little of why, a password needs to be changed regularly. In addition, the organization may be helped of they are educated about typical security breaches that can occur. Technical staff will need more in-depth education about preventing security problems from occurring, solving unexpected security problems and reporting them to the appropriate people.

b. Traditional-age Students vs. Returning Adult Students

Students in an educational program are typically one of two types, the traditional-age student progressing through the academic process, as we have come to expect, and the returning adult student with several years of work experience. In most instances they are seeking the same result, entry into the information security field, either applied or research. At times they may co-exist in a program. However, typically specific part-time programs are usually offered for the returning adult student. These programs are not usually considered when issues concerning education are addressed.